METHOD FOR SIGNALLING IN A SIGNALLING TRANSFER POINT

Routing loops

It can occur in signalling networks ~~according to~~ that are based on signalling system No. 7 ~~that routing loops occur in the network~~ on MTP level 3 due to incorrect planning or operating ~~errors, so that messages are~~ errors. This results in messages being routed to one or more destinations in a loop without ever reaching their destination. Of particular interest here are loops having a length greater than 2 ("length of a loop" means the plurality of signalling points participating in a loop) ~~and, in particular, how such loops can be eliminated when they are recognized.~~ detection and elimination of

If loops potentially present in the tables are in fact used for routing, ~~thus represents~~ occurs. Since a serious problem for the network ~~since~~ messages, on the one hand, do not arrive at their destination and, on the other hand, ~~use~~ consume valuable resources of the network. ~~It should therefore be~~ Thus, loops should be detected and eliminated as fast as possible.

Loops having the length 2 (so-called ping-pong loops) ~~cannot~~ are unlikely to occur given a functioning protocol in the MTP (message transfer point). Should they nonetheless arise, these loops can be easily ~~recognized~~ detected in real time in a signalling transfer point when ~~that~~ being a check is carried out to see whether a message is ~~to be~~ routed over the same linkset on which it was received. ~~They are just as easy to correct in that~~ These are simple to correct when the unsuccessful protocol actions (sending transfer prohibited -- TFP -- messages to the cooperating party) are repeated.

Loops having a length of more than 2 are more difficult to ~~recognize~~ detect. A check can in fact be performed with every message in a specific STP as to whether this message derives from precisely this STP (by comparing the OPC (originating point code) contained in the message to the PointCode of the STP). When this ~~is the case,~~ happens there is a loop in the network. STPs, however, do not necessarily generate messages or, ~~respectively~~, do not necessarily generate messages to the destination or destinations to which there is a loop.

This problem can be solved by a real-time method that recognizes the possibility of a loop, for example due to a lasting overload on a linkset. When ~~said~~ this method recognizes the possibility of a loop, the ~~operating personnel~~ operators can be informed so that corrective measures can be initiated.

The standard (Q.753, Q.754) defines another solution of the problem, ~~what is referred to~~ as the MTP route verification test (MRVT), ~~that checks all possible~~ paths in an MTP network between two given points for correctness, including ~~freedom from~~ loops. Upon occurrence of errors such as, for example, loops, the ~~operating personnel~~ ~~is~~ informed ~~in order to undertake~~ corrections. MRVT in fact has the advantage over a real-time method that it can ~~also recognize~~ loops before they are actually ~~used, since~~ all possible paths are checked, not only the current ones. The disadvantage, however, is that a separate protocol is required ~~for it~~. When this is not realized ~~in~~ the entire network, the check is not possible or is only possible in incomplete form. This situation is specifically established in the international signalling network. ~~Due~~ to the load that it generates, ~~moreover~~, the MRVT cannot constantly check all routes between all points in the network.

The invention is based on the object of overcoming the ~~aforementioned~~ disadvantages.

This object is achieved by a method according to claim 1.

~~The invention is explained in greater detail below with the assistance of the drawing, whereby the drawing comprises 3 Figures.~~

~~Figure 1 shows an example of a loop.~~

~~Figures 2 and 3 shows methods for parting a loop.~~

The present invention particularly reveals how, given real-time recognition of loops having a length ~~>~~ 2 and/or upon recognition of loops by the MRVT, the loops can be broken by automatic, real-time, protocol-compatible methods that are simple to realize. ~~The time elapsing before the operating personal takes action can thus be bridged.~~

~~It must thereby be mentioned that it is advantageous, given *possible* loops~~ that were ~~recognized~~ by the MRVT or a real-time method for a linkset, to check ~~before having potential recourse to~~ automatic correction measures (the MRVT, namely, does not supply any statements whether a possible loop is also being employed at the time and, under certain circumstances, the real-time method cannot make any statements about the destination to which a possible loop is present). ~~Said~~ check ensues by sending otherwise unemployed MTP network management messages

to the destinations that can be reached (according to the routing) via the ~~appertaining~~ pertinent linkset. When such test messages return to the STP, these messages are detected by comparing the OPC contained in the message to the point code of the STP, and ~~if~~ loops ~~or, respectively, several loops are recognized. Correction measures can thereby~~ remain limited to loops being currently ~~employed~~ selected.

~~Said~~ This check with the assistance of test messages is ~~already~~ useful when it is ~~realized in only one STP~~ applied in only one STP, since all loops that run through this STP can be ~~recognized~~ detected. The check method can also always ~~be~~ remain active.

Another possibility is ~~comprised~~ based on in making the initiation of correction measures dependent ~~of~~ on the evaluation of the (relative) probability that the possible loop could be ~~employed~~ selected. These information can be made available by the MRVT in the form of priorities of the individual paths constituting the loop.

When a loop to a destination X is ~~recognized~~ detected in an STP A by the MRVT or by real-time methods, one can proceed in the following way for breaking the loop:

a) Breaking the loop "downstream" in that the specific departing path to this destination is blocked in the routing table in A. This step can, in particular, be ~~implemented when other paths to X are also available proceeding from A. In this case, it is recommendable~~ it is recommended to also check the route ~~employed~~ selected as an alternative for the occurrence of a loop. Although the lack of a detection of a loop ~~is no~~ does not guarantee that there is not some other loop that ~~no longer~~ does not contains A, there is at least a probability that the problem has been eliminated.

b) Alternatively, or if, for example, there no longer happens to be an alternate (loop-free) route proceeding from A, the loop can be broken "upstream", i.e. to the preceding STP B on the loop, in that A sends B a transfer prohibited message with respect to X. In response ~~thereto~~, B will reroute or, ~~respectively~~, stop the traffic to X. Since B will subsequently and periodically review the availability of the route to X via A with what are referred to as route set messages, it must be assured that A does not answer these messages with a transfer allowed, since B could otherwise re-close the loops.

After final correction of the routing tables by the ~~operating personnel~~ operators, the actions automatically undertaken by the MTP or the operations maintenance and administration part (OMAP) can be in turn reversed by the operating personnel (Note:

OMAP comprises higher-ranking SS7 management functions, for example MRVT, screening functions and measurements. "Informing the operating personnel" is also (partially) part of the OMAP).

~~A special characteristic~~ Another aspect of the invention is ~~comprised in~~ the mechanism for breaking up loops having ~~the~~ a length more than 2 with automatic measures that are simple to realize ~~upon utilization of~~ when the existing protocol features are applied. In particular, the method ~~can already be employed~~ and is useful when it is realized in only a single STP.

One possibility for realizing the alternative (b) is to automatically activate what is referred to as ILS/DPC screening (ILS = incoming linkset; see Q.705, §8) in A for messages from B to X. However, a linking of the ILS/DPC screening into the MTP management network is needed for this purpose such that an illegal message is answered with a TFP message and also that the route set test messages are ~~also~~ correctly handled.

Add A11